Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer				IHK-Nummer			Prüflingsnummer				
6	9	1	2	0	2							
Sp. 1-2		Sp. 3-6				Sp. 7-9			Sp. 10-14			

Termin: Mittwoch, 7. Mai 2025

IHK

Abschlussprüfung Sommer 2025

1202

1 Konzeption und Administration von IT-Systemen

Fachinformatiker
Fachinformatikerin
Systemintegration

Teil 2 der Abschlussprüfung

4 Aufgaben
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg. ☐☐ (15 16) Punkte 2. Aufg. ☐☐ (17 18) Punkte 3. Aufg. ☐☐ (19 20) Punkte 4. Aufg. ☐☐ (21 22) Punkte

Prüfungszeit ☐ (23)
Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Gesamtpunktzahl ☐☐☐ (24 25 26)

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und

Korrekturrand

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie sind bei der Retailer GmbH als Fachinformatiker für Systemintegration beschäftigt. Die Retailer GmbH ist ein mittelständisches Unternehmen im Bereich Logistik. Die IT-Systeme der Retailer GmbH werden laufend weiterentwickelt.

In diesem Zusammenhang sollen Sie die folgenden vier Aufgaben bearbeiten:
1. IT-Systeme planen und konfigurieren
2. Die Verfügbarkeit der Dienste sicherstellen
3. Mobile Endgeräte verwalten
4. Systemsoftware entwickeln

1. Aufgabe (26 Punkte)

Die Retailer GmbH benötigt aus Kapazitätsgründen eine leistungsstärkere Plattform für den E-Mail-Dienst.

a) Der E-Mail-Dienst lief bislang auf einem physischen Server.

aa) Sie sollen prüfen, inwieweit es für die Retailer GmbH vorteilhaft ist, den E-Mail-Dienst in einer virtuellen Maschine zu betreiben.

Erläutern Sie je drei Vorteile und Nachteile einer Virtualisierung von Servern. 6 Punkte

Vorteile einer Virtualisierung:

Nachteile einer Virtualisierung:

ab) Zur weiteren Entscheidungsfindung über eine eventuelle Virtualisierung des E-Mail-Dienstes sollen Sie über den Typ-1-Hypervisor und über den Typ-2-Hypervisor informieren.

Ergänzen Sie dazu die Tabelle. 8 Punkte

	Typ-1-Hypervisor (native oder bare-metal)	**Typ-2-Hypervisor (gehostet)**
Erläutern Sie kurz den jeweiligen Hypervisor-Typ.		
Geben Sie für die beiden Hypervisor-Typen je ein sinnvolles Einsatzbeispiel an.		
Geben Sie für die beiden Hypervisor-Typen je ein marktgängiges Produkt an.		

Korrekturrand

b) Für die Datenspeicherung wird zurzeit ein RAID-6-Verbund mit einer Nettospeicherkapazität von 80 TiB verwendet. Die Nettospeicherkapazität des RAID-6-Verbunds soll verdoppelt werden. Im RAID-6-Verbund sind Festplatten mit einer Kapazität von je 8 TiB verbaut.

ba) Berechnen Sie nachvollziehbar, wie viele Festplatten mit einer Kapazität von je 8 TiB für die Erweiterung des RAID-6-Verbunds auf 160 TiB benötigt werden. 2 Punkte

bb) Im Zuge der Erweiterung des RAID-Verbunds wird die Sicherheit der Daten gegen Verlust bei einem Festplattenausfall in einem RAID-10-Verbund und in einem RAID-6-Verbund verglichen.

Erläutern Sie den Sachverhalt am Beispiel eines gleichzeitigen Ausfalls von zwei Festplatten. 3 Punkte

bc) Als weiteres Entscheidungskriterium für einen möglichen Wechsel von RAID 6 auf RAID 10 soll die jeweils verfügbare Nettospeicherkapazität betrachtet werden.

Berechnen Sie nachvollziehbar die Nettospeicherkapazität für einen RAID-10-Verbund mit der Anzahl Festplatten des erweiterten RAID-6-Verbunds aus ba). 2 Punkte

Hinweis: Sollten Sie ba) nicht bearbeitet haben, gehen Sie von zwölf Festplatten für die Erweiterung des RAID 6 aus.

c) Die Server der Retailer GmbH haben zusammen eine maximale Leistungsaufnahme von 600 VA. Diese sind an eine USV mit einer Ausgangsleistung von 2.400 VA angeschlossen. Bei vollständig geladenen Akkus kann die USV die Server rechnerisch 60 Minuten lang mit Strom versorgen.

Bei Stromausfall soll zunächst die USV die Server so lange mit Strom versorgen, bis die Akkuladung auf 30 % abgesunken ist. Dann soll ein Notstromaggregat die Stromversorgung der Server übernehmen. Das Notstromaggregat benötigt vom Start bis zur vollständigen Betriebsbereitschaft drei Minuten.

Berechnen Sie nachvollziehbar, bei welchem prozentualen Ladungsstand der Start des Notstromaggregates eingeleitet werden muss. 5 Punkte

2. Aufgabe (27 Punkte)

Korrekturrand

Bei der Retailer GmbH ist es Angreifern gelungen, firmenkritische Daten – einschließlich Kundeninformationen – im SAN zu verschlüsseln. Sie wirken an der Untersuchung des Vorfalls und der Datenwiederherstellung mit. Anschließend sollen Sie Maßnahmen zur Verbesserung der IT-Sicherheit vorschlagen.

a) Erste Analysen deuten darauf hin, dass es sich gemäß DSGVO um einen erheblichen IT-Sicherheitsvorfall handelt. In solchen Fällen ist zu prüfen, ob die betroffenen Kunden darüber informiert werden müssen.

Nennen Sie drei datenschutzrelevante Kriterien, die darüber entscheiden, ob eine Information erfolgen muss. 3 Punkte

b) Originale der kompromittierten Daten liegen in einem kürzlich erstellten Voll-Backup auf einem LTO-Medium vor.

Die Wiederherstellung der Daten vom Bandlaufwerk dauert mehr als acht Stunden. Daten, die seit dem letzten Backup neu erstellt wurden, können nicht wiederhergestellt werden. Dies verursacht erhebliche wirtschaftliche Schäden für die Retailer GmbH.

Um Derartiges zukünftig auszuschließen, sollen Sie einen Vorschlag zur Verkürzung der erforderlichen Zeit für die Datenwiederherstellung und einen Vorschlag zur Vermeidung des Verlusts noch nicht gesicherter Daten ausarbeiten und erläutern.

6 Punkte

Verkürzung der Zeit für die Datenwiederherstellung:

Vermeidung von Datenverlust:

c) Bei der Weiterentwicklung des Datensicherungskonzepts soll auch die 3-2-1-Regel für Backups berücksichtigt werden.

Entwickeln Sie einen dieser Regel entsprechenden Vorschlag für die Datenhaltung bei der Retailer GmbH und erläutern Sie diesen. 4 Punkte

Korrekturrand

d) Aufgrund des stattgefundenen IT-Sicherheitsvorfalls sollen umgehend Schutzmaßnahmen eingeleitet werden. Die IT-Sicherheit der Server und Clients soll durch eine „System-Härtung" verbessert werden.
Dazu zählen Maßnahmen, wie z. B. die Sicherstellung der Aktualität der installierten Software.

Erläutern Sie zwei weitere Maßnahmen, die einer „System-Härtung" dienen. 4 Punkte

e) Sicherheitsexperten empfehlen im Rahmen von Sicherheitskonzepten für IT-Systeme folgende Prinzipien: Das Least-Privilege-Prinzip und das Zero-Trust-Prinzip.

Beide Prinzipien sollen bei der Retailer GmbH implementiert werden.

Erläutern Sie zu jedem Prinzip eine typische Maßnahme. 6 Punkte

Least-Privilege-Prinzip

Zero-Trust-Prinzip

f) Die Wirksamkeit der umgesetzten Maßnahmen soll von einem Sicherheits-Dienstleister getestet werden. Dieser bietet an, folgende Tests durchzuführen:

- Den aktuellen Patch-Stand ermitteln
- Passwort- und Benutzersicherheit prüfen
- Fehlkonfigurationen in IT-Systemen aufspüren
- Fehlkonfigurationen im Active-Directory aufspüren

Beschreiben Sie zwei zusätzliche sicherheitsrelevante Tests, die noch eingefordert werden sollten. 4 Punkte

3. Aufgabe (22 Punkte)

Korrekturrand

Die Retailer GmbH will ein „Mobile Device Management System" (MDMS) zur effizienten Administration der mobilen Endgeräte einführen.

a) Es liegt die folgende tabellarische Übersicht der Leistungsmerkmale von drei MDM-Systemen vor.

Leistungsmerkmal	Anbieter A	Anbieter B	Anbieter C
Unterstützte Clients	IOS/Android/Windows	IOS/Android/Windows	Android/Windows
Unterstützte Plattformen	On Premises/Public Cloud/ Hybrid Cloud	On Premises/Public Cloud/ Hybrid Cloud	Public Cloud
Logs und Reports	**Ja**	**Ja**	**Ja**
Content-Management-System	**Nein**	**Nein**	**Ja**
Black- und Whitelisting	**Ja**	**Ja**	**Ja**
Bring your own Device	**Ja**	**Ja**	**Ja**
Client-Ortung	**Ja**	**Ja**	**Ja**
Wipe Mobile Device	**Ja**	**Nein**	**Ja**
Lockdown Mobile Device	**Ja**	**Ja**	**Nein**
E-Mail-Management	**Ja**	**Ja**	**Ja**
Eigener App-Store	**Nein**	**Ja**	**Nein**
Kamera Zugriffssteuerung	**Ja**	**Ja**	**Ja**
Geräteinventarisierung	**Ja**	**Ja**	**Ja**
MDMS-Profile	**Ja**	**Ja**	**Ja**
Software-Updates	**Ja**	**Ja**	**Ja**

aa) Wählen Sie den Anbieter aus, dessen MDMS bei Verlust oder Diebstahl eines mobilen Gerätes den besten Schutz gegen missbräuchliche Nutzung bietet und begründen Sie Ihre Entscheidung. 4 Punkte

ab) Die Retailer GmbH erlaubt ihren Mitarbeitern die Nutzung privater Endgeräte für dienstliche Zwecke, sofern diese in das MDMS eingebunden sind.

Beschreiben Sie, wie der Schutz privater Daten auf einem Endgerät gegenüber dem MDMS sichergestellt wird. 2 Punkte

ac) Die Retailer GmbH will eine Betriebsvereinbarung zur Nutzung mobiler Endgeräte mit dem Betriebsrat abschließen. Sie sollen technische und/oder organisatorische Sachverhalte vorschlagen, die Bestandteil einer solchen Vereinbarung sein sollten.

Korrekturrand

Zwei Sachverhalte wurden bereits vorgeschlagen:

- Verschlüsselung von Daten bzw. Datenträgern
- Private Nutzung der Geräte

Nennen Sie fünf weitere Sachverhalte. 5 Punkte

b) Für den Zugriff auf den MDMS-Server sind auch Client-Zugriffs-Lizenzen (CAL) erforderlich. Angeboten werden die zwei im Folgenden beschriebenen Lizenztypen.

Erläutern Sie für jeden der beiden beschriebenen Lizenztypen den kostengünstigeren Einsatzfall. 6 Punkte

User CAL: Companies purchase a user CAL for each user who accesses the MDMS-Server. Purchasing a user CAL makes sense if the company's employees uses multiple devices or if there are simply more devices than users in the company.

Device CAL: Companies purchase a device CAL for each device that accesses the MDMS-Server, regardless of the number of users that use that device to access the server. It can make more economic and administrative sense for employees to share devices within the company.

c) Die Aktualisierung des MDMS erfolgt, wie auch bei anderen Softwareprodukten üblich, in Form von „Updates" und „Upgrades".

Erläutern Sie den Unterschied zwischen „Update" und „Upgrade" mit Blick auf Kosten und Funktion. 5 Punkte

4. Aufgabe (25 Punkte)

Korrekturrand

Sie wirken bei der Erstellung von Programmen zur Systemverwaltung mit und sollen folgende, aus prüfungstechnischen Gründen stark vereinfachte, Aufgabe bearbeiten.

a) Ein Array mit der Bezeichnung „RAM1" enthält neun Felder. Die Anzahl Felder ist nicht mehr ausreichend und soll verdoppelt werden. Da keine entsprechende Methode zum Vergrößern eines Arrays existiert, soll ein neues entsprechend großes Array mit der Bezeichnung „RAM2" angelegt werden. Der Inhalt von Array „RAM1" soll nach Array RAM2" entsprechend dem folgenden Schema kopiert werden. Die weiteren Felder des Arrays „RAM2" sollen mit den im Schema angegebenen Zahlen (1, 2, 3 ...) gefüllt werden.

Schema:

RAM1	40	42	47	52	50	60	64	66	71									
RAM2	1	40	2	42	3	47	4	52	5	50	6	60	7	64	8	66	9	71
[Index]	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Folgender Programmentwurf liegt vor:

```
int[] RAM1 = new int[9] { 40, 42, 47, 52, 50, 60, 64, 66, 71 };
int[] RAM2 = new int[18];
for (int i = 0; i < 9; i++)
   {
      RAM2[i * 2 + 1] = i;
      RAM2[i * 2] = RAM1[i];
   }
```

aa) Analysieren Sie den Programmentwurf. Stellen Sie fest, welche Werte in den ersten neun Feldern von „RAM2" gespeichert werden.

Tragen Sie die Werte in die vorgesehenen Felder ein. 9 Punkte

RAM2									
[Index]	0	1	2	3	4	5	6	7	8

ab) Offensichtlich liefert das Programm falsche Werte. Dafür sind zwei Fehler im Programmcode verantwortlich.

Lokalisieren Sie die beiden Fehler und geben Sie zu jedem Fehler den korrekten Code an. 10 Punkte

Korrekter Code 1

Korrekter Code 2

b) Fehler, die beim Programmieren vorkommen, werden unterschieden in Syntaxfehler und in Semantikfehler.

Beschreiben Sie die beiden Fehlerarten und geben Sie dazu jeweils ein Beispiel an. 6 Punkte

Syntaxfehler:

Semantikfehler:

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

[1] Sie hätte kürzer sein können.
[2] Sie war angemessen.
[3] Sie hätte länger sein müssen.

Abschlussprüfung Sommer 2025
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

1 Konzeption und Administration von IT-Systemen

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=		100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2025 – Alle Rechte vorbehalten!

1. Aufgabe (26 Punkte)

aa) 6 Punkte (2 x 3 Punkte)

Vorteile von Virtualisierung:

- Geringer Energieverbrauch
- Effiziente Ressourcennutzung
- Schnelles Backup und Restore
- Isolierte Applikationen
- Schnelle Server-Provisionierung
- Ältere Anwendungen möglich
- u. a.

Nachteile von Virtualisierung:

- Erfordert leistungsstarke Hardware
- Erfordert geeignete (zertifizierte) Hardware
- Leistungseinbußen durch Ressourcen-Sharing
- Single Point of Failure
- Virtualisierungs-Software erforderlich
- Komplexität der Administration erhöht sich
- Gefahr von „Side-Channel"-Angriffen
- u. a

ab) 8 Punkte

2 Punkte je Erläuterung, 1 Punkt je Beispiel

	Hypervisor-Typ-1 (native oder bare-metal)	**Hypervisor-Typ-2 (gehostet)**
Erläutern Sie kurz den jeweiligen Hypervisor-Typ.	Die Virtualisierungs-Software setzt direkt auf der Hardware-Ebene auf und hat somit direkten Zugriff auf die Hardware-Ressourcen.	Die Virtualisierungs-Software läuft auf einem bereits installierten Betriebssystem und verhält sich insgesamt wie ein Anwendungsprogramm.
Geben Sie für die beiden Typen ein sinnvolles Einsatzbeispiel an.	Überwiegend zur Bereitstellung von Server-diensten. u. a.	Überwiegend im Bereich von Arbeitsplätzen zur Entwicklung und zum Test von Software. u.a.
Geben Sie für die beiden Typen ein marktgängiges Produkt an.	Microsoft Hyper-V VMware vSphere KVM u. a.	VMware Workstation Oracle VirtualBox Parallels u. a.

ba) 2 Punkte

Es werden **zehn Festplatten** für die Erweiterung benötigt. Rechenwege sind nicht verlangt.

12 Festplatten sind vorhanden
80 TiB / 8 TiB für die Daten, also 10 Festplatten
2 Festplatten als Paritätsplatten
zusammen 12 Festplatten

22 Festplatten werden insgesamt benötigt
20 Festplatten für die Daten (160 TiB / 8 TiB)
2 Festplatten für die doppelte Redundanz
zusammen 22 Festplatten (20 + 2)

10 Festplatten zusätzlich (22 Festplatten – 12 Festplatten)

bb) 3 Punkte

RAID 6 bietet einen Schutz gegen Datenverlust bei bis zu zwei gleichzeitig defekten Festplatten. (1 Punkt)

RAID 10 schützt zuverlässig nur gegen den Ausfall einer Festplatte. Abhängig davon, welche Festplatten ausfallen, kann die Anzahl defekter Festplatten auch größer sein. (2 Punkte)

bc) 2 Punkte
Es sind **88 TiB** Nettospeicherkapazität bei RAID 10 möglich.

22 Festplatten verfügbar, die Hälfte ist nutzbar (22 / 2 = 11)
11 Festplatten * 8 TiB = 88 TiB

Wurde mit einem falschen Wert aus ab) richtig weitergerechnet sind entsprechend Punkte zu vergeben.

Alternativ mit Vorgabewert:
Es sind **96 TiB** Nettospeicherkapazität bei RAID 10 möglich.
Anzahl Festplatten vor der Erweiterung = 12
Anzahl Festplatten Vorgabewert = 12
Summe Festplatten = 24
Nettospeicherkapazität = (24 / 2) * 8 TiB) = 96 TiB

c) 5 Punkte
Bei einem Ladungszustand von **35 %** muss das Notstromaggregat gestartet werden.

60 min entsprechen 100 %
1 % entspricht 0,6 min
5 % entsprechen 3 min (Startzeit)
30 % + 5 % = 35 %

2. Aufgabe (27 Punkte)

a) 3 Punkte
- Sind die Daten an Unbefugte gelangt
- Können die Daten wiederhergestellt werden
- Sind die Daten verändert worden
- Sind die Daten missbräuchlich verwendet worden
- Waren die Daten durch Verschlüsselung geschützt
- u. a.

b) 6 Punkte (2 x 3 Punkte)
Zeit für die Datenwiederherstellung verkürzen:
Um den hohen Zeitbedarf für die Rücksicherung der Backup-Daten vom Bandlaufwerk (LTO) zu vermeiden, sollten die Backup-Daten zunächst auf ein dafür besonders geeignetes Speichermedium (Festplatte) geschrieben werden. In einem zweiten Schritt wird im Hintergrund auf ein Bandlaufwerk gesichert. Dies entspricht dem Konzept Disk-to-Disk-to-Tape-Backup (D2D2T-Backup).
Die Datenwiederherstellung vom Speichermedium (Festplatte) ist wesentlich schneller, das Bandlaufwerk kann zusätzlich eingesetzt werden.

Datenverlust vermeiden:
Das Durchführen von inkrementellen Datensicherungen auf einem Speichermedium (Festplatte) in kurzen Zeitabständen.

oder

Um einen Datenverlust zu vermeiden, der zwischen zwei Backups möglich ist, sollten in kurzen Zeitabständen Snapshots durchgeführt werden.

Andere richtige Antworten sind möglich.

c) 4 Punkte
Die 3-2-1-Regel besagt, dass die Daten mindestens 3-fach (Originaldaten und zwei Kopien) gespeichert sein sollen. Für die Speicherung sollen mindestens zwei verschiedene Medien (z. B. Festplatte, Bandlaufwerk, Cloud) verwendet werden. Davon soll eine Kopie der Daten an einem entfernten Standort in sicherer Umgebung verwahrt werden.

d) 4 Punkte
Bei der Härtung eines IT-Systems werden u. a. folgende Maßnahmen durchgeführt:

Überprüfen von:
- Laufen Dienste nur mit den zwingend notwendigen Rechten
- Der Notwendigkeit eines aktivierten Dienstes
- Kann der Dienst in einer isolierten Umgebung laufen
- Sind Wartungsschnittstellen und -zugänge gesperrt
- Ist der Zugriff auf die Konfigurationsdateien des Betriebssystems gesperrt
- Anpassung aller vorhandenen Standard-Kennwörter entsprechend einer unternehmensinternen Kennwort-Richtlinie

Deaktivierung von:
- Fehler- oder Debug-Meldungen für Endbenutzer
- Unsicheren, veralteten und/oder nicht benötigten Schnittstellen
- Nicht benötigten Autostart-Mechanismen
- Unnötigen Betriebssystem-Komponenten
- Unnötigen Hintergrund-Diensten

Aktivierung:
- Eines Bildschirmschoners mit Kennwort-Schutz
- Starker Benutzerkontensteuerung (User Account Control)
- Des Antiviren-Programms beim Start des Betriebssystems
- Umfangreiche Protokollierung von Systemereignissen
- Der CPU-Sicherheitsfunktionen
- Des BIOS-Zugriffspasswortes
- Einer festgelegten Boot-Reihenfolge
- u. a.

e) 6 Punkte (2 x 3 Punkte)
Das **Least-Privilege-Prinzip** verfolgt in der IT den Ansatz, Personen und Maschinen nur die Rechte/Berechtigungen einzuräumen, die für die Erledigung der Aufgaben mindestens erforderlich sind. Dadurch soll ein möglicher Missbrauch verhindert werden.

Das **Zero-Trust-Prinzip** verfolgt den Ansatz, innerhalb eines lokalen Firmennetzes ständig den Zugriff der Systeme untereinander zu überwachen.
So soll die Ausbreitung von Schadsoftware zwischen den IT-Systemen verhindert werden.

f) 4 Punkte
- Logs auswerten
- Login-Versuche für bekannte Accounts durchführen (Brute Force)
- Prüfen der Sicherheit der Applikationen
- Prüfen der Sicherheit der Dienste
- Prüfen gemäß Richtlinienvorgaben (BSI bzw. firmenintern)
- Prüfen aller Clients auf Malware
- u. a.

3. Aufgabe (22 Punkte)

aa) 4 Punkte
Die Wahl fällt auf Anbieter A, da nur dieser die entsprechenden Sicherheits-Features wie „Lockdown Mobile Device“ und „Wipe Mobile Device“ anbietet, die laut Aufgabenbeschreibung gefordert werden.

ab) 2 Punkte
Die Client-Software des MDMS läuft auf den mobilen Endgeräten als Container-Anwendung. Der MDMS-Client hat somit keine Rechte/Berechtigungen für den privaten Bereich des Endgerätes. Der Zugang zum MDMS-Client ist passwortgeschützt, um die Sicherheit der Firmendaten zu gewährleisten.

Andere fachlich richtige Antworten möglich.

ac) 5 Punkte
- Passwortrichtlinien
- Regelung zu BYOD
- Private Nutzung von dienstlichen Geräten
- Klassifizierung von Daten in Schutzklassen
- Schutzbedarfsanalyse
- Erfassung und Speicherung von Bewegungsdaten
- Schulung von Mitarbeitern
- Rechte-/Berechtigungsvergabe
- Fernsteuerung der Kamera
- u. a.

b) 6 Punkte (2 x 3 Punkte)
User CALs (Nutzer-CALs):
Für jeden Nutzer wird eine Lizenz benötigt, um die Funktionen des MDMS nutzen zu können.
Nutzer-CALs sind dann sinnvoll, wenn die Mitarbeiter des Unternehmens an verschiedenen Geräten oder mit mehreren Geräten arbeiten.

Device CALs (Geräte-CALs):
Device CALs sind Geräte bezogen. Für jedes Gerät wird eine Lizenz benötigt, um das MDMS nutzen zu können. Arbeiten mehrere Nutzer an einem Gerät (z. B. Schichtbetrieb), kann die Anzahl benötigter Lizenzen geringer sein als die Anzahl der Nutzer.

c) 5 Punkte
Ein Update dient der schnellen Behebung von Software-Fehlern und dem Schließen von Sicherheitslücken. Es entstehen keine Kosten. In der Regel werden auch keine Änderungen am Funktionsumfang vorgenommen.

Upgrades werden in größeren Zeitabständen angeboten als Updates. In einem Upgrade sind oft Erweiterungen des Funktionsumfangs und neue Sicherheitskonzepte enthalten. In vielen Fällen entstehen für ein Software-Upgrade auch Kosten.

Andere fachlich richtige Antworten sind möglich.

4. Aufgabe (25 Punkte)

aa) 9 Punkte (Teilpunkte je nach Ansatz vergeben, Verschiebung der Zahlen, Unvollständigkeit usw.)

RAM2	**40**	**1**	**42**	**2**	**47**	**3**	**52**	**4**	**50**
[Index]	0	1	2	3	4	5	6	7	8

ab) 10 Punkte (5 Punkte je Code)
Korrekter Code 1
```
RAM2[i * 2] = i + 1;
```

Korrekter Code 2
```
RAM2[i * 2 + 1] = RAM1[i];
```

Andere funktional richtige Vorschläge sind möglich. Teilpunkte je nach Ansatz vergeben.

b) 6 Punkte (2 x 3 Punkte)
Syntaxfehler:
Syntaxfehler verstoßen gegen die Definitionen/Grammatik bezüglich der Schreibweise im Programmcode.
Beispielsweise: „innt" statt „int", oder „array()" statt „array[]" oder Semikolon vergessen.

Semantikfehler:
Semantikfehler führen zu falschen Ergebnissen bei der Programmausführung. Beispielsweise wird das Ergebnis in einer anderen Variablen gespeichert als beabsichtigt: statt in „Umfang" in „Flaeche".

Andere zutreffende Erläuterungen und Beispiele sind auch als richtig zu bewerten.